Google Inc. et al v. Egger et al Doc. 440

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (CSB No. 145997)
cindy@eff.org
LEE TIEN (CSB No. 148216)
KURT OPSAHL (CSB No. 191303)
KEVIN S. BANKSTON (CSB No. 217026)
CORYNNE MCSHERRY (CSB No. 221504)
JAMES S. TYRE (CSB No. 083117)
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

LAW OFFICE OF RICHARD R. WIEBE
RICHARD R. WIEBE (CSB No. 121156)
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382

FENWICK & WEST LLP
LAURENCE F. PULGRAM (CSB No. 115163)
lpulgram@fenwick.com
JENNIFER KELLY (CSB No. 193416)
CANDACE MOREY (CSB No. 233081)
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350

Attorneys for Amici

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION, MDL No. 1791 This Document Relates To: Al-Haramain Islamic Foundation, et al., v. Bush, et al. (07-CV-0109-VRW)	MDL Docket No 06-1791 VRW **AMICI CURIAE MEMORANDUM OF MDL PLAINTIFFS ADDRESSING THE APPLICATION OF THE PROTOCOL OF SECTION 1806(f), TITLE 50 U.S.C., TO CIVIL ACTIONS FOR UNLAWFUL ELECTRONIC SURVEILLANCE** Date: April 23, 2008 Time: 10:00 a.m. Courtroom: 6, 17th Floor Judge: The Hon. Vaughn R. Walker

Dockets.Justia.com

TABLE OF CONTENTS

INTRODUCTION **1**

ARGUMENT **1**

I. THE FIVE-STEP PROTOCOL OF SECTION 1806(F) PERMITS COURTS TO RESOLVE THE MERITS OF CIVIL ACTIONS ALLEGING UNLAWFUL SURVEILLANCE 1

II. CONGRESS ENACTED THE SECTION 1806(F) PROTOCOL AND THE CIVIL LIABILITY PROVISIONS OF FISA AS PART OF ITS EFFORT TO CURB MASSIVE DRAGNET SURVEILLANCE BY THE EXECUTIVE 4

A. Before FISA, The Executive Branch Routinely Abused Its Power When Conducting Electronic Surveillance For National Security Purposes 5

B. Revelations Leading Up to Formation of the Church Committee 5

C. The Church Committee's Findings That Intelligence Agencies Had Engaged in Massive Spying Abuses 6

D. Congress Passed FISA To End The Executive's Abuse Of Warrantless Surveillance In The Name Of National Security 8

E. Congress Intended For The Judiciary To Play A Significant Oversight Role In the Executive's Electronic Surveillance Activities 9

III. WHENEVER THE GOVERNMENT SEEKS TO PROTECT FROM DISCLOSURE INFORMATION RELATING TO ELECTRONIC SURVEILLANCE ON GROUNDS OF HARM TO THE NATIONAL SECURITY, IT MUST INVOKE THE SECTION 1806(F) PROTOCOL 11

A. Congress Intended For Section 1806(f) To Apply To Civil As Well As Criminal Cases 11

B. It Is The Government, Not The Party Seeking Discovery, That Triggers Section 1806(f) By Contending That Disclosure Of Information Regarding Surveillance Would Cause Harm To The National Security 13

C. Section 1806(f) Applies To All Causes Of Action In Which The Lawfulness Of Electronic Surveillance Is At Issue 17

D. Use Of Section 1806(f)'s Protocol To Decide The Legality Of Massive, Suspicionless Dragnet Surveillance Will Not Threaten National Security 17

IV. THE GOVERNMENT'S NOTION THAT SECTION 1806(F) DOES NOT SPEAK DIRECTLY TO THE USE OF EVIDENCE THAT WOULD OTHERWISE BE SUBJECT TO THE STATE SECRETS PRIVILEGE IS MERITLESS 20

V. CONGRESS HAS THE AUTHORITY TO REGULATE THE USE IN LITIGATION OF INFORMATION THAT THE EXECUTIVE ASSERTS IS A STATE SECRET 23

CONCLUSION **25**

TABLE OF AUTHORITIES

CASES

ACLU v. Barr, 952 F.2d 457 (1991) 4, 17
Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190 (9th Cir. 2007) 21
Hamdan v. Rumsfeld, 126 S.Ct. 2749, 2773 (2006) 24, 25
Hamdi v. Rumsfeld, 542 U.S. 507 (2004) 25
Hepting v. AT&T Corp., 439 F.Supp.2d 974 (N.D. Cal. 2006) .... passim
In re Evans, 452 F.2d 1239 (D.C. Cir. 1971) 16
Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998) 21, 22, 23
Little v. Barreme, 6 U.S. 170 (1804) 24
Masalosalo v. Stonewall Ins. Co., 718 F.2d 955 (9th Cir. 1983) 18
Plotkin v. Pacific Tel. and Tel. Co. 688 F.2d 1291 (9th Cir. 1982) 18
U.S. v. Stanley, 483 U.S. 669 (1987) 18
U.S. v. Vielguth, 502 F.2d 1257 (9th Cir. 1974) 16
U.S. v. Yanagita, 552 F.2d 940 (2d Cir. 1977) 16
Yamaha Motor Corp. v. Calhoun, 516 U.S. 199 (1996) 18
Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952) 8, 24, 25

STATUTES

18 U.S.C. § 2510(8) 17
18 U.S.C. § 2511(2)(a)(ii)(B) 19
18 U.S.C. § 2511(f) 9, 12
18 U.S.C. § 2712(b)(4) 13
18 U.S.C. § 3504 .... 15, 16
28 U.S.C. § 1292(b) 17
50 U.S.C. § 1801 9
50 U.S.C. § 1801(f)(2) 17
50 U.S.C. § 1801(f)(2) 18
50 U.S.C. § 1801(k) 16

50 U.S.C. § 1801(n) 17
50 U.S.C. § 1804 9
50 U.S.C. § 1806(c) 2
50 U.S.C. § 1806(e) 2
50 U.S.C. § 1806(f) .... passim
50 U.S.C. §1806(d) 2
Fed. R. Civ. Pro. 26(b)(1) 14
Foreign Intelligence Surveillance Act of 1978, Pub .L. 95-511, 92 Stat. 1783 .... 4, 9

CONSTITUTIONAL PROVISIONS

Const. art. I, § 8, cl. 12 24
Const. art. I, § 8, cl. 18 24
Const. art. I, § 8, cl. 9 24
Const. art. III, § 1 24
Const., art. I,§ 8, cl. 14 24

LEGISLATIVE MATERIALS

116 Cong. Rec., 91st Cong., 2nd Sess. 5
124 Cong. Rec. 28427, 28431 at § 106(g) 15
Electronic Surveillance for National Security Purposes: Hearings Before the Subcomm. on Criminal Laws and Procedures and Constitutional Rights, 93rd Cong. (1974) 10
Foreign Intelligence Surveillance Act of 1977, Hearings on S. 1566 Before the Subcomm. On Criminal Laws and Procedures of the Senate Comm. on the Judiciary, 95th Cong. (1977). 10, 15
H.R. Conf. Rep. No. 95-1720 (1978)*, reprinted in* 1978 U.S.C.C.A.N. 4048 13
H.R. Rep. No. 95-1283 (1978) 10
S. Rep. No. 110-209 at 10 (2007) 19
S. Rep. No. 94-1035 (1976) 10
S. Rep. No. 95-604(I) (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904 .... 8, 10
S. Rep. No. 95-701 (1978) *reprinted in* 1978 U.S.C.C.A.N. 3973 .... 14, 15
Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities,

("Church Committee Reports"), Book II*: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755 (1976) *available at* http://www.aarclibrary.org/publib/church/reports/book2/contents.htm....................................6, 7, 8

Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee Reports"), Book III: *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755 (1976), *available at* http://www.aarclibrary.org/publib/church/reports/book3/contents.htm 6, 7

OTHER AUTHORITIES

Athan Theoharis, *Spying on Americans: Political Surveillance From Hoover To the Huston Plan* 120 (1978) 7

Christopher H. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, Wash. Monthly, January 1970.. 5

James Bamford, *The Puzzle Palace* 303 (1983)... 7

Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L. Rev. 1306 (2004).. 9

Seymour Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. Times, Dec. 21, 1974.. 5, 6

Siobhan Gorman, *NSA's Domestic Spying Grows as Agency Sweeps Up Data*, Wall St. J., Mar. 10, 2008..20

INTRODUCTION

The government's motion to dismiss pending before this Court in the Al-Haramain action raises the general question posed to the Court by the Ninth Circuit in its remand in *Al-Haramain v. Bush*: whether section 1806(f) of title 50 U.S.C. preempts the state secrets privilege and, in civil actions alleging unlawful surveillance, permits the use by the Court, under appropriate security precautions, of materials relating to electronic surveillance whose disclosure might harm the national security. This is a general question that permeates all of the MDL actions, not just the Al-Haramain action, and it is one in which the MDL plaintiffs joining in this brief all have an interest.[1]

In section 1806(f), Congress after much deliberation crafted a careful protocol specifically designed to address the question of how a court should proceed to determine the lawfulness of electronic surveillance in a civil action once the government asserts that disclosures of materials relating to the surveillance would harm the national security. Section 1806(f) lays out a detailed, five-step protocol that directs the court to make its determination of lawfulness by using an in camera proceeding to consider the materials relating to the surveillance. Because section 1806(f) preempts the state secrets privilege, in unlawful surveillance civil actions when the government makes an assertion that harm to the national security would result from the disclosure of evidence, the evidence is not excluded and the court proceeds forward under section 1806(f) to a determination of the merits.

ARGUMENT

I. The Five-Step Protocol Of Section 1806(f) Permits Courts To Resolve The Merits Of Civil Actions Alleging Unlawful Surveillance

As always, the appropriate starting point is the statutory language itself. Section 1806(f) of title 50 U.S.C. (hereafter "section 1806(f)" or "§ 1806(f)") has two sentences. The first sentence of section 1806(f) begins by describing the three categories of events to which the section applies (we have added indentations and line breaks for ease of reading):

---

[1] This amici memorandum is joined in by the plaintiffs identified on the signature page.

> "Whenever a court or other authority
>
> [i] is notified pursuant to subsection (c) or (d) of this section, or
>
> [ii] whenever a motion is made pursuant to subsection (e) of this section, or
>
> [iii] whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any state
>
> to discover or obtain applications or orders or other materials relating to electronic surveillance or
>
> to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, . . ."

§ 1806(f) (bracketed numbers added). The first two categories are not relevant to civil actions for unlawful surveillance; the first arises when the federal or a state government intends to use surveillance evidence against a person in a judicial or administrative proceeding (§§ 1806(c); 1806(d)), and the second arises when a person against whom the government has said it intends to use surveillance evidence moves to suppress that evidence (§ 1806(e)).

It is the third category, and the first prong under that category, that are relevant here. The plaintiff in an unlawful surveillance civil action is entitled to make a "request," pursuant to the discovery provisions of the Federal Rules, "to discover or obtain applications or orders or other materials relating to electronic surveillance." By doing so, the plaintiff opens the door to the government to assert its interest in secrecy through the section 1806(f) protocol, as follows:

> "the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority,
>
> shall,
>
> notwithstanding any other law,
>
> if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States,
>
> review in camera and ex parte
>
> the application, order, and such other materials relating to the surveillance as may be necessary
>
> to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted."

§ 1806(f) (line breaks added for clarity). Thus, if in response to any of the three categories of events, the Attorney General triggers section 1806(f) by contesting the disclosure of "the application, order, and such other materials relating to the surveillance" as harmful to the national security, section 1806(f) directs that the Court, "notwithstanding any other law," "shall" proceed to review the "materials relating to the surveillance" and "determine whether the surveillance of the aggrieved person was lawfully authorized and conducted."

Section 1806(f) concludes with a separate provision in its second sentence authorizing disclosure to the surveilled person, under appropriate security procedures, where necessary to assist in the court in making an accurate determination of the legality of the surveillance:

> In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

§ 1806(f).

The provisions of section 1806(f) relevant to unlawful surveillance civil actions can be condensed as follows:

> … whenever *any motion or request* is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court … of the United States … to discover or obtain applications or orders or other *materials relating to electronic surveillance* … the United States district court … shall, *notwithstanding any other law*, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, *review in camera and ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to *determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.* In making this determination, *the court may disclose to the aggrieved person*, under appropriate security procedures and protective orders, portions of *the application, order, or other materials* relating to the surveillance *only* where such disclosure is *necessary to make an accurate determination of the legality* of the surveillance.

§ 1806(f) (emphasis added).

In section 1806(f), Congress thus laid out a five-step protocol for the Executive and the Judiciary alike to follow whenever, in civil litigation over the lawfulness of electronic surveillance like the MDL actions, the Executive resists on national security grounds a request for disclosure of materials related to the electronic surveillance. The five-step protocol is as follows:

1. The protocol begins with a “motion or request . . . by an aggrieved person . . . to discover or obtain . . . materials relating to electronic surveillance.” § 1806(f).

2. Once that request comes, in camera, ex parte proceedings are triggered if in response “the Attorney General [then] files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States.” *Id.*

3. Upon receipt of that affidavit, the “court . . . shall, notwithstanding any other law, . . . review in camera and ex parte” any materials relating to the surveillance “as may be necessary [to allow the court] to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” *Id.* This provision authorizes the court to review not just the specific materials requested by the plaintiff but also any other materials “necessary” to its determination.

4. Based upon that submission, the court decides whether to “disclose to the aggrieved person” any “materials relating to the surveillance”—a step that is permissible “only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.” *Id.*

5. If the court concludes that disclosure to the plaintiff is necessary, the court discloses the materials under “appropriate security procedures and protective orders” to protect against any national security risk. *Id.*

In the end, whether or not the materials relating to the surveillance are disclosed to the plaintiff, the Court must “determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” *Id.*; *ACLU v. Barr*, 952 F.2d 457, 462, 465 & n.7 (1991).

Section 1806(f) was enacted in 1978 as part of the original FISA statute. Pub. L. No. 95-511, § 106(f); 92 Stat. 1783, 1794. It has not been amended since. FISA’s civil liability provision, section 1810, was also enacted in 1978 as part of the original FISA statute. Pub. L. No. 95-511, § 110; 92 Stat. 1783, 1796. It, too, has never been amended.

II. Congress Enacted The Section 1806(f) Protocol And The Civil Liability Provisions Of FISA As Part Of Its Effort To Curb Massive Dragnet Surveillance By The Executive

Given the dispositive clarity of the statutory text, the government makes only a few half-hearted textual arguments against section 1806(f)’s application to civil actions. Instead, the government argues that Congress did not intend for section 1806(f) to apply according to its plain terms. As the context in which Congress acted in 1978 when it enacted FISA makes clear, Congress intended to authorize civil actions seeking relief from unlawful surveillance, even in cases where the government asserts that evidence relating to the surveillance must be kept secret.

A. Before FISA, The Executive Branch Routinely Abused Its Power When Conducting Electronic Surveillance For National Security Purposes

In the years leading up to passage of FISA in 1978, it came to light that the National Security Agency (NSA), Federal Bureau of Intelligence (FBI) and Central Intelligence Agency (CIA) secretly had been monitoring the communications and activities of millions of innocent Americans—without warrants or other legal authorization, and in many cases for reasons that had nothing to do with national security—for nearly *five* decades. These massive surveillance abuses were unearthed in the 1970s by the press and by a congressional committee formed to investigate and address the lack of oversight of intelligence activities being conducted by the Executive.

B. Revelations Leading Up to Formation of the Church Committee

In the early 1970s, a series of startling allegations began to surface, starting with allegations that the U.S. Army had been spying on the civilian population and keeping records of their domestic political activities in a secret database under a program dubbed CONUS. Christopher H. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, Wash. Monthly, January 1970, at 4, *reprinted in* 116 Cong. Rec. 2227 (1970). According to Pyle, the Army began CONUS in 1965 to gather logistical information for use during civil disturbances, but the program morphed over the years as the Army began spying on political activities and "maintain[ing] files on the membership, ideology, programs, and practices of virtually every political activist group in the country." *Ibid.* The public outcry that followed prompted the Senate Subcommittee on Constitutional Rights to investigate the alleged spying program with public hearings to investigate "the dangers the Army's program presents to the principles of the Constitution." 116 Cong. Rec. 26329 (1970).

Then came a cascade of revelations that, since the 1950s, the CIA had been engaging in illegal and unauthorized domestic operations that included wiretapping and physical surveillance of reporters and investigative journalists, opening of citizens' mail to and from selected countries, and amassing files on 9,900-plus Americans related to their opposition to the Vietnam War. Memorandum for the File: CIA Matters, James A. Wilderotter, Assoc. Dep. Atty. Gen. (Jan. 3, 1975). Investigative journalist Seymour Hersh reported that:

> The Central Intelligence Agency, directly violating its charter, conducted a massive, illegal domestic intelligence operation during the Nixon Administration against the

> antiwar movement and other dissident groups in the United States, according to well-placed Government sources.

Seymour Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. Times, Dec. 21, 1974, at 1.

Congress formed the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities on January 27, 1975. Known informally as the "Church Committee," after its Chairman, Senator Frank Church, the bipartisan committee was tasked with conducting a comprehensive investigation of intelligence gathering by agencies controlled by the Executive, and making a recommendation as to any needed reforms.

C. The Church Committee's Findings That Intelligence Agencies Had Engaged in Massive Spying Abuses

The Church Committee's in-depth investigation of intelligence activities revealed that the government had been spying on American citizens, without warrants or other legal authorization, for decades. S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, ("Church Committee Reports"), Book II*: Intelligence Activities and the Rights of Americans* ("Book II"), S. Rep. No. 94-755 at 12 (1976) (concluding that "surveillance was often conducted by illegal or improper means").[2]

As the Church Committee found, successive Attorneys General consistently interpreted the Federal Communications Act of 1934 (the "1934 Act") to allow wiretapping as long as no information was shared outside the government. Book II at 36. This "questionable interpretation" (*ibid.*) eliminated any judicial or legislative oversight of the Executive's surveillance activities.

Moreover, the Church Committee found that there was a "steady increase in the government's capability and willingness to pry into, and even disrupt, the political activities and personal lives of the people." Book II at 21. Eventually intelligence activity began targeting organizations and citizens engaged in constitutionally protected political speech and activities. *Id.* at 22; *see also* Church Committee Reports, Book III: *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* ("Book III") at 4-5, 81, 174.

---

[2] The Church Committee reports are available online at http://www.aarclibrary.org/publib/church/reports/contents.htm.

The Church Committee also uncovered a massive espionage program operated by the NSA, known as SHAMROCK, which bears disturbing similarity to the NSA's warrantless surveillance programs at issue in these actions. As the Committee found:

> SHAMROCK is the code-name for a special program in which the NSA received copies of most international telegrams leaving the United States between August 1945 and May 1975. Two of the participating international telegraph companies—RCA Global and ITT World Communications—provided virtually all their international message traffic to NSA. The third, Western Union International, only provided copies of certain foreign traffic from 1945 until 1972. SHAMROCK was probably the largest governmental interception program affecting Americans ever undertaken. Although the total number of telegrams read during its course is not available, NSA estimates that in the last two or three years of SHAMROCK's existence, about 150,000 telegrams per month were reviewed by NSA analysts.

Book III at 765.[3] The NSA disseminated the information collected through SHAMROCK to other governmental agencies, including the FBI and the CIA. *Id*. at 735.

Then—as now, over thirty years later—the intelligence agencies sought to justify their dragnet warrantless surveillance activities by invoking "national security" and "foreign intelligence." Book II at 205, 208. The Committee was greatly troubled by this, observing that:

> [A]pplication of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment rights of both the targets and those with whom the targets communicated.

Book III at 332. The Committee concluded SHAMROCK likely violated the Fourth Amendment, as well as the 1934 Act and the controlling National Security Council Directive. *Id.* at 755-66.

The Church Committee ultimately concluded that "the massive record of intelligence abuses over the years" had "undermined the constitutional rights of citizens … primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied." Book II at 290, 289. The Committee urged "fundamental reform" (*id*.), recommending legislation to "make clear to the Executive branch that [Congress] will not condone, and does not accept, any theory of inherent or implied authority to violate the Constitution, the proposed new charters, or any other statutes." *Id*. at 297. Citing *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), it noted that "[c]ertainly, there would be no such authority after Congress has … covered the field by enactment of a comprehensive legislative charter" that would "provide the exclusive legal authority for domestic security activities," including "warrantless electronic surveillance." Book II at 297 & n.10. The Committee also recommended creation of civil remedies for unlawful surveillance and anticipated the protocol of section 1806(f), stating that "courts will be able to fashion discovery procedures, including inspections of materials in chambers, and to issue orders as the interests of justice require, to allow plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest." *Id*. at 337.

---

[3] The telegraph companies initially were hesitant to participate in SHAMROCK, fearing the program violated the 1934 Act's ban on wiretapping and that their participation could subject them to criminal prosecution. James Bamford, *The Puzzle Palace* 303 (1983). Company executives therefore conditioned their cooperation in the program upon receiving either assurances of immunity from criminal prosecution or clear congressional authorization of the program. Athan Theoharis, *Spying on Americans: Political Surveillance From Hoover To the Huston Plan* 120 (1978). Choosing the path that would shield their conduct from judicial or legislative scrutiny, the Executive opted to promise the telegraph companies immunity from prosecution. Bamford, at 303.

D. Congress Passed FISA To End The Executive's Abuse Of Warrantless Surveillance In The Name Of National Security

FISA was Congress' response to the Church Committee's revelations that "warrantless electronic surveillance in the name of national security has been seriously abused." S. Rep. No. 95-604(I) at 7 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908.[4] A "precisely drawn legislative charter" (Book II at 309), FISA reflects Congress' intent to restore balance between the protection of civil liberties and the protection of the national security by providing "effective, reasonable safeguards to ensure accountability and prevent improper surveillance" by the Executive. S. Rep. No. 95-604(I) at 7.[5]

To fulfill this intent, Congress expressly provided in FISA that FISA and the domestic law

[4] Much of FISA's legislative history is available online at http://www.cnss.org/fisa.htm and is discussed in the Brief of Amicus Curiae People for the American Way Foundation in Support of Plaintiffs-Appellees, *Hepting v. AT&T*, Nos. 06-17132, 06-17137 (9th Cir. filed May 3, 2007).

[5] As Senator Kennedy stated in introducing the bill that ultimately became FISA: "The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens. Our objective has been to reach some kind of balance that will protect the security of the United States without infringing on our citizens' human liberties and rights." S. Rep. No. 94-1035 at 11.

enforcement electronic surveillance provisions of title 18 (originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968) are the exclusive means by which the Executive may conduct electronic surveillance within the United States:

> [T]he procedures in this chapter [chapter 119 of title 18, the codification of Title III] and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 of such Act [50 U.S.C. § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted.

Pub. L. No. 95-511; 92 Stat. at 1794 (emphasis added); *codified at* 18 U.S.C. § 2511(2)(f). FISA created a comprehensive set of procedural and substantive restraints on conducting electronic surveillance activities for foreign intelligence purposes, including setting up the Foreign Intelligence Surveillance Court (the "FISC") to authorize such surveillance. 50 U.S.C. § 1801 *et seq*. FISA permits surveillance of American citizens and others only where the FISC determines, upon a showing of probable cause, that the target is an "agent of a foreign power" as defined in the statute. *Id*. at § 1801(b). FISA also provides for criminal and civil liability against those who conduct electronic surveillance in violation of the statute. *Id*. at §§ 1809, 1810.

Congress has amended FISA several times since it was passed in 1978, including via the USA Patriot Act in 2001. *See* Pub. L. No. 107-56. Yet the procedural and substantive framework Congress originally created remains intact—including the Judiciary's role in reviewing the legality of the Executive's surveillance activities, both *ex ante* and *ex post*, civil liability for unlawful surveillance, and the precisely drawn protocol of section 1806(f) governing how sensitive information pertaining to the national security is to be handled in litigation. *See* Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L. Rev. 1306, 1312 (2004).

E. Congress Intended For The Judiciary To Play A Significant Oversight Role In the Executive's Electronic Surveillance Activities

Through FISA, Congress expressly empowered the Judiciary to review the legality of the government's electronic surveillance activities in two ways. First, FISA provides for judicial review of electronic surveillance *before* it may be initiated. *See* 50 U.S.C. § 1804 (requiring that intelligence officers obtain a warrant from the FISC before commencing surveillance). Second, FISA authorizes the courts to review the legality of governmental surveillance activities *after* they have occurred, substantively by creating civil liability for unlawful electronic surveillance (50 U.S.C. § 1810) and procedurally by creating the five-step protocol of section 1806(f).

From the very inception of the legislative process, Congress made clear its view that the Executive's unchecked assertion of a right to conduct electronic surveillance in the name of "national security" must end. *E.g.*, S. Rep. No. 95-604(I) at 8, 1978 U.S.C.C.A.N. at 3910 (stating that the bill was designed "to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it"); S. Rep. No. 94-1035 at 11 (1976) ("the past record establishes clearly that the executive branch cannot be the sole or final arbiter of when such proper circumstances exist"), 20 (noting that the bill "is based on the premise (supported by history), that executive self-restraint, in the area of national security electronic surveillance, is neither feasible nor wise").

Congress determined that the Judiciary was the appropriate body to exercise oversight. Both the House and the Senate considered the same arguments the government now raises here: the Judiciary is ill-suited for this oversight role because of judges' alleged lack of experience in matters of foreign policy and national security, and the national security will be harmed if secret information pertaining to matters of national security is used in litigation, even in camera and ex parte. *See*, *e.g.*, *Electronic Surveillance for National Security Purposes*, *Hearings Before the Subcomms. on Criminal Laws and Procedures and Constitutional Rights of the S. Comm. on the Judiciary*, 93rd Cong., 255 (1974); H.R. Rep. No. 95-1283 at 25 (1978).

These arguments were soundly rejected by a strong majority in Congress. The legislative record is replete with expressions of Congress' firm view that the government's need for secrecy in matters of national security simply did *not* trump the need for judicial oversight of its electronic surveillance activities. *See* S. Rep. No. 94-1035 at 79 ("We believe that these same issues—secrecy and emergency, judicial competence and purpose—do not call for any different result in the case of foreign intelligence collection through electronic surveillance."); *Foreign Intelligence Surveillance Act of 1977, Hearings on S. 1566 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary*, 95th Cong., at 2728 (1977) (Attorney General Bell asserting that "[t]he most leakproof branch of the Government is the judiciary…. I have seen intelligence matters in the courts…. I have great confidence in the courts," and Senator Orrin Hatch replying, "I do also.").

Instead, Congress addressed the concern that the national security could be harmed if matters relating to the government's electronic surveillance activities were publicly disclosed, while still preserving the safeguard of civil liability for those, including telecommunications carriers, who participate in unlawful surveillance, by carefully crafting a comprehensive protocol to deal with sensitive information. That protocol is section 1806(f).

III. Whenever The Government Seeks To Protect From Disclosure Information Relating To Electronic Surveillance On Grounds Of Harm To The National Security, It Must Invoke The Section 1806(f) Protocol

Congress intended section 1806(f) to provide an exclusive protocol for the government to use to protect against harm to the national security in both civil and criminal cases in which the lawfulness of electronic surveillance is at issue, while providing courts with a mechanism for determining whether the surveillance was lawful.

A. Congress Intended For Section 1806(f) To Apply To Civil As Well As Criminal Cases

The government suggests that section 1806(f) is limited to the government's use of surveillance evidence "against" an aggrieved person in a criminal case (e.g., Motion at 13:3) and does not apply when the government asserts that disclosure of information relating to electronic surveillance sought by civil plaintiffs will harm the national security. This suggestion is contrary to the text of the statute, the statutory scheme, and the legislative history.

As explained in Section I(A) above, section 1806(f) applies to three distinct categories of events. Only the first two of these categories involve the government's use of surveillance evidence against a person. The third category contains no such limitation, but applies "whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States … to discover or obtain applications or orders or other materials relating to electronic surveillance." § 1806(f).

This makes sense given FISA's statutory scheme as a whole. Because the government and the telecommunications carrier are the only ones aware that covert electronic surveillance is occurring, Congress recognized that telecommunications carriers had a critical role to play in keeping the government honest and making sure that the only electronic surveillance that occurs is that authorized by FISA and Title III, i.e., that FISA and Title III remain the "exclusive means" by which surveillance is conducted. 18 U.S.C. § 2511(f). Telecommunications carriers would have no incentive to play this role and stand up to unlawful requests by the government, however, unless they were individually liable for unlawful surveillance. So Congress in 18 U.S.C. § 2520 and 50 U.S.C. § 1810 made telecommunications carriers and others who participate in unlawful electronic surveillance civilly liable as a central means for enforcing the exclusivity of FISA and Title III. Congress completed the statutory scheme by providing the section 1806(f) protocol as the practical means by which the civil liability necessary to protect the exclusivity of FISA and Title III could be enforced without endangering the national security.

The legislative history also confirms that section 1806(f) applies to civil cases. The Senate and the House of Representatives in 1978 passed two different FISA bills, each with a different version of the provision that became section 1806(f), before ultimately reaching agreement on the FISA bill that was enacted into law. The Senate bill provided a single protocol for determining the legality of electronic surveillance in both criminal and civil cases. The House bill had two separate protocols for determining the legality of electronic surveillance: One House protocol applied to criminal cases where the government sought to use surveillance evidence against an aggrieved person, i.e., the first two categories of the enacted version of section 1806(f). The other House protocol applied to civil cases in which a determination of the legality of the surveillance was at issue, i.e., the third category of the enacted version of section 1806(f). The two House protocols had different standards for disclosure to the aggrieved person, among other differences.

The report of the joint House and Senate Committee of Conference for the enacted version of FISA describes the Senate and House versions and their differences as follows:

> The Senate bill provided a single procedure for determining the legality of electronic surveillance in a subsequent in camera and ex parte proceeding …. The Senate bill also provided that, in making this determination, the court should disclose to the aggrieved person materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

> The House amendments provided two separate procedures of determining the legality of electronic surveillance …. In criminal cases, there would be an in camera proceeding; and the court might disclose to the aggrieved person … materials relating to the surveillance if there were a reasonable question as to the legality of the surveillance and if disclosure would promote a more accurate determination of such legality, or if disclosure would not harm the national security. In civil suits, there would be an in camera and ex parte proceeding before a court of appeals; and the court would disclose … to the aggrieved person or his attorney materials relating to the surveillance only if necessary to afford due process to the aggrieved person.

H.R. Conf. Rep. No. 95-1720 at 31-32 (1978)*, reprinted in* 1978 U.S.C.C.A.N. 4048, 4060-61 ("FISA Conf. Comm. Rep.").

In the end, Congress adopted a modified version of the Senate protocol, deeming a single protocol sufficient both for criminal cases in which the aggrieved person was seeking to suppress surveillance evidence the government intended to use against him or her and for civil cases in which the aggrieved person was seeking a determination of the legality of electronic surveillance:

> The conferees agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance *in both criminal and civil cases*.

FISA Conf. Comm. Rep. at 32, 1978 U.S.C.C.A.N. at 4061 (emphasis added); *see also* 18 U.S.C. § 2712(b)(4) (As part of the congressionally mandated process for litigating FISA and wiretapping claims against the United States, Congress directed, "[n]otwithstanding any other provision of law," that the procedures set forth in section 1806(f), along with similar provisions in sections 1825(g) and 1845(f), are the "exclusive means by which certain materials may be reviewed.")

This legislative history shows that Congress repeatedly and in detail considered how best to structure the protocol for determining the legality of surveillance in a way that accommodates both the interests of national security and the need for due process and the rule of law. Congress deliberately chose to make section 1806(f) available not just to criminal defendants facing the use of electronic surveillance evidence against them, but to civil plaintiffs seeking vindication of constitutional and statutory rights violated by unlawful surveillance.

B. It Is The Government, Not The Party Seeking Discovery, That Triggers Section 1806(f) By Contending That Disclosure Of Information Regarding Surveillance Would Cause Harm To The National Security

The government argues that section 1806(f) only applies if the persons who are seeking discovery relating to electronic surveillance are persons whom the government has already acknowledged it has surveilled. This argument lacks merit.

First, the government looks at section 1806(f) through the wrong end of the telescope. It is the government, not the party seeking information relating to electronic surveillance, that triggers section 1806(f) by, for example, responding to a discovery request with the assertion that the disclosure of information would harm the national security. Section 1806(f) is not "invoked by parties seeking to discover" materials, contrary to the government's contention (Motion at 16); rather, it is invoked by the Attorney General's notification to the court "that disclosure or an adversary hearing would harm the national security." § 1806(f); S. Rep. No. 95-701 at 63 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032 ("The special procedures … cannot be invoked until they are triggered by a Government affidavit that disclosure or an adversary hearing would harm the national security …. If no such assertion is made, the committee envisions … mandatory disclosure ….."); FISA Conf. Rep. at 32 ("The in camera and ex parte proceeding is invoked if the Attorney General files an affidavit under oath.").

A civil plaintiff seeking discovery of information relating to electronic surveillance does not need to prove that the surveillance actually occurred before making the discovery request, any more than any other party in any other action needs to prove up its case before seeking discovery. Nothing in the section 1806(f) process requires the plaintiff to prove he or she has been surveilled before seeking discovery. Instead, as in any other case, the right to seek discovery requires nothing more than a complaint whose allegations, including allegations of standing, are sufficiently robust to withstand a motion to dismiss, and a connection of relevance between the discovery requested and the "claim or defense of any party," Fed. R. Civ. Pro. 26(b)(1). Invocation of section 1806(f) rests in the hands of the government, the same party that knows whether or not the plaintiff is aggrieved; otherwise, the case proceeds as usual.

Second, the government's argument is fatally flawed because it rests on portions of Senate Intelligence Committee Report No. 95-701 that discuss the suppression of illegal surveillance evidence in criminal trials. Motion at 19-20 & n.19. The portions of the report that the government relies on discussing the suppression of evidence, however, pertain to a version of Senate bill 1566 whose protocol for the in camera, ex parte review of surveillance materials was significantly different from the protocol that was ultimately enacted as section 1806(f).

In the Senate Intelligence Committee version of Senate bill 1566 that Senate Report No. 95-701 discusses, the third category of the protocol consisted entirely of: "… or whenever any motion or request is made by an aggrieved person pursuant to section 3504 of this title [18] or any other statute or rule of the United States, to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance …." S. 1566, 95th Cong. (as reported by S. Select Comm. on Intelligence, Mar. 14, 1978). In that earlier bill, unlike the enacted version of FISA, the third category of the protocol was limited to what is now its second prong in section 1806(f), the one that permits aggrieved persons "to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance." § 1806(f). This second prong, which does pertain to motions to suppress surveillance evidence itself, i.e., the contents of what was overheard, is *not* the prong applicable to the evidence sought by the Al-Haramian plaintiffs or the other MDL plaintiffs. *See* Opposition at 16. The bill had not yet been broadened to include as well the first prong of the third category of section 1806(f), the prong that applies when a civil plaintiff seeks "to discover or obtain applications or orders or other materials relating to electronic surveillance." § 1806(f). It is this first prong, not addressed by the Senate Report on which the government relies, that applies to the evidence sought by the Al-Haramain plaintiffs and the other MDL plaintiffs.[6]

Third, it was established at the time FISA was enacted that a person was "aggrieved" by electronic surveillance if the person had a colorable basis for believing he or she had been surveilled. Even in the narrower Senate Intelligence Committee version of Senate bill 1566 set forth above, "motion[s] or request[s] made by an aggrieved person" included motions under 18 U.S.C. § 3504. S. 1566, 95th Cong. (as reported by S. Select Comm. on Intelligence, Mar. 14, 1978); *see also* S. Rep. No. 95-701 at 63, 1978 U.S.C.C.A.N. at 4032 ("This procedure applies, for example, whenever an individual makes a motion … pursuant to … 18 U.S.C. 3504 …."). Section

[6] The first prong of the third category was added later by the House to the version of Senate bill 1566 that the House passed September 7, 1978. 124 Cong. Rec. 28427, 28431 at § 106(g) (S. 1566 as reported by the House September 7, 1978). As explained above, the House and Senate versions of Senate bill 1566, and their differing provisions regarding the section 1806(f) protocol, were then reconciled by the Committee of Conference into the final version of FISA that Congress enacted.

3504, enacted in 1970, is a statute that permits a "party aggrieved" who claims that evidence is inadmissible because it is the fruit of an illegal electronic surveillance to require the government to "affirm or deny the occurrence of the alleged unlawful act" of surveillance. 18 U.S.C. § 3504. At the time FISA was enacted, it was established that a party was "aggrieved" and entitled to discovery from the government under section 3504 so long as the party could state a colorable basis for believing he or she had been subjected to electronic surveillance. *U.S. v. Vielguth*, 502 F.2d 1257, 1258 (9th Cir. 1974) ("the government's obligation to affirm or deny the occurrence of electronic surveillance under section 3504(a)(1) 'is triggered . . . by the mere assertion that unlawful wiretapping has been used against a party.' "); *In re Evans*, 452 F.2d 1239, 1247 (D.C. Cir. 1971) (same); *U.S. v. Yanagita*, 552 F.2d 940, 943 (2d Cir. 1977) (surveillance allegations that have a " 'colorable' basis … function to trigger the government's obligation to respond under § 3504"). Because section 3504 motions are within the scope of section 1806(f), persons with a colorable basis for alleging they have been surveilled (a standard the MDL plaintiffs exceed by a wide margin) are "aggrieved persons" for purposes of section 1806(f).

Finally, the government's position ignores the fact that a plaintiff may well be able to establish the fact of surveillance even absent an acknowledgment by the government. Nothing in 50 U.S.C. § 1801(k)'s definition of "aggrieved person" refers to a government acknowledgment of surveillance. Not only Al-Haramain but the other cases before the Court in this MDL proceeding provide good examples of independent evidence disclosing that plaintiffs have been surveilled. The Hepting action, for example, has already progressed beyond mere allegations of electronic surveillance and has established an unrebutted factual basis demonstrating that plaintiffs have been surveilled. "AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content." *Hepting v. AT&T Corp.*, 439 F.Supp.2d 974, 991-92 (N.D. Cal. 2006). "In opposing a subsequent summary judgment motion, plaintiffs could rely on many non-classified materials including present and future public disclosures of the government or AT&T on the alleged NSA programs, the AT&T documents and the supporting Klein and Marcus declarations and information gathered during discovery." *Id.* at 998. "The court further notes that the AT&T documents and the accompanying Klein and Marcus declarations provide at least some factual basis for plaintiffs' standing." *Id.* at 1001. Other MDL plaintiffs have a similarly rich lode of disclosure to support their claims. *See*, *e.g.*, Dkt. # 315 at 2-13, 23-31 in 06-1791 (discussing evidence applicable to MCI and Verizon).

C. Section 1806(f) Applies To All Causes Of Action In Which The Lawfulness Of Electronic Surveillance Is At Issue

The five-step protocol of section 1806(f) applies to all statutory and constitutional claims of unlawful surveillance, not just claims for FISA violations. Section 1806(f) is not limited to certain classes of claims. "When a district court conducts a § 1806(f) review, its task is not simply to decide whether the surveillance complied with FISA. Section 1806(f) requires the court to decide whether the surveillance was 'lawfully authorized and conducted.'" *Barr*, 952 F.2d at 465; *id.* at 465 n.7. Section 1806(f) provides, without qualification, that it applies to all "electronic surveillance," which is defined to encompass any "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication … without the consent of any party thereto." 50 U.S.C. § 1801(f)(2). The protocol also covers communications records because "contents" is defined to include "any information concerning the *identity of the parties* to such communication or the *existence* … of that communication." 50 U.S.C. § 1801(n) (emphasis added); *cf.* 18 U.S.C. § 2510(8) (narrower definition of contents for purposes of Wiretap Act). Information concerning disclosure of communications records is also subject to section 1806(f) because such information is "material[] relating to the surveillance." § 1806(f).

D. Use Of Section 1806(f)'s Protocol To Decide The Legality Of Massive, Suspicionless Dragnet Surveillance Will Not Threaten National Security

Because section 1806(f) applies to all "electronic surveillance," it applies not only to targeted surveillance claims but also to claims of untargeted surveillance like those of many of the MDL plaintiffs.[7] Untargeted surveillance falls under subsection (2) of the definition of "electronic

---

[7] At the February 7, 2008 CMC, counsel for AT&T suggested that the pendency of the Hepting appeal somehow limited the Court's ability to take a broad view of section 1806(f) in the course of deciding the government's motion in Al-Haramain. This suggestion is entirely erroneous.

First, the Hepting interlocutory appeal is taken under 28 U.S.C. § 1292(b), which strictly limits appellate jurisdiction to the issues actually decided in the certified order on appeal. On a section 1292(b) appeal, " 'the scope of the issues open to the court of appeals is closely limited to the order surveillance" in 50 U.S.C. section 1801(f): "(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, …." 50 U.S.C. § 1801(f)(2). (Targeted electronic surveillance of "a particular, known United States person" is described in subsection (1) of the definition of "electronic surveillance".)

Many of the MDL plaintiffs allege massive, untargeted, suspicionless dragnet surveillance of millions of ordinary Americans. This surveillance is *not* targeted at any individual plaintiff, *not* based on any indicia of suspicion that any plaintiff has any connection to terrorists or terrorist activity, and *not* authorized by any court order or lawful FISA certification.

Untargeted dragnet surveillance limits both the scope and the detail of the "materials relating to the surveillance" necessary to prove a plaintiff's claims. To decide an untargeted dragnet surveillance claim, it is not necessary for a court to intrusively examine intelligence sources and methods, for by definition the government does not have any grounds for suspicion, and thus has not relied on any intelligence sources and methods in conducting the surveillance. Whatever post-acquisition sifting and winnowing the government may do later on whatever basis is irrelevant to a plaintiff's untargeted dragnet surveillance claim, and need not be reviewed by the

---

appealed from.' " *U.S. v. Stanley*, 483 U.S. 669, 677 (1987). "The court of appeals may not reach beyond the certified order" and may address only those "issue[s] fairly included within the certified order." *Yamaha Motor Corp. v. Calhoun*, 516 U.S. 199, 205 (1996).

Here, however, the Court in its *Hepting* Order expressly *refrained* from reaching or deciding the issue of whether section 1806(f) preempts the state secrets privilege. *Hepting*, 439 F.Supp.2d at 998 ("the court declines to address these issues presently"). Thus, the pendency of the Hepting appeal is no obstacle to the Court reaching a conclusion that section 1806(f) preempts the state secrets privilege with respect to the subject matter of materials and information relating to electronic surveillance in civil actions seeking relief from unlawful surveillance. *Plotkin v. Pacific Tel. and Tel. Co.* 688 F.2d 1291 (9th Cir. 1982) ("an appeal from an interlocutory order does not divest the trial court of jurisdiction to continue with other phases of the case").

Second, even as to those matters decided by a certified order on appeal, the "rule of exclusive appellate jurisdiction is a creature of judicial prudence, however, and is not absolute. It is designed to avoid the confusion and inefficiency of two courts considering the same issues simultaneously." *Masalosalo v. Stonewall Ins.*, 718 F.2d 955, 956 (9th Cir. 1983) (citation omitted). Here, the Ninth Circuit has made clear in its Al-Haramain remand that it will not be deciding the section 1806(f) preemption question and that it wants this Court to go forward and decide it in the first instance.

court to determine the lawfulness of the surveillance.

As the Court noted in *Hepting*, "AT&T incorrectly focuses on whether plaintiffs have pled that the government 'monitored [plaintiffs'] communications or records or targeted [plaintiffs] or their communications.' Instead, the proper focus is on AT&T's actions. Plaintiffs' statutory claims stem from injuries caused solely by AT&T through its alleged interception, disclosure, use, divulgence and/or publication of plaintiffs' communications or communication records…. Hence, plaintiffs need not allege any facts regarding the government's conduct to state these claims." *Hepting*, 439 F.Supp.2d at 999.

Moreover, as the Court anticipated in its *Hepting* Order, disclosures relating to the electronic surveillance of the MDL plaintiffs have continued apace. The Senate Intelligence Committee has reviewed the letters the Executive provided to the telecommunications carriers in connection with its warrantless electronic surveillance of plaintiffs, and its disclosure of the letters' contents confirms that they do not conform to the requirements of 18 U.S.C. § 2511(2)(a)(ii)(B) for electronic surveillance without a court order. Section 2511(2)(a)(ii)(B) requires "a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required."

The Intelligence Committee report states:

> The Committee has reviewed all of the relevant correspondence. The letters were provided to electronic communication service providers at regular intervals. All of the letters stated that the activities had been authorized by the President. All of the letters also stated that the activities had been determined to be lawful by the Attorney General, except for one letter that covered a period of less than sixty days. That letter, which like all the others stated that the activities had been authorized by the President, stated that the activities had been determined to be lawful by the Counsel to the President.

S. Rep. No. 110-209 at 10 (2007).

Obviously missing from the letters to the telecommunications carriers are the required representations "that no warrant or court order is required by law [and] that all statutory requirements have been met"—the heart of section 2511(2)(a)(ii)(B)'s immunity. The representation in the letters that "the activities had been determined to be lawful by the Attorney

General" is no substitute for section 2511(2)(a)(ii)(B)'s requirements. The contents of the letters that the Senate Intelligence Committee has already disclosed provide a basis for litigating the issue of the lawfulness of the authorization the telecommunications carriers received, and section 1806(f) provides a mechanism for review by the Court of additional "materials relating to the surveillance" should that prove necessary. In its *Hepting* Order, the Court anticipated that just such a redacted version of any authorization the defendants are relying on would be adequate to adjudicate any certification-based defense. *Hepting*, 439 F.Supp.2d at 996-97. Section 2511(2)(a)(ii) of title 18, moreover, permits a telecommunications carrier to disclose a certification "as may … be required by legal process."

Even more recently, in the latest of many continuing disclosures in the press, the Wall Street Journal offered further confirmation of the NSA's ongoing massive, suspicionless dragnet surveillance. Siobhan Gorman, *NSA's Domestic Spying Grows as Agency Sweeps Up Data*, Wall St. J., Mar. 10, 2008, p. A1.[8] The article confirms the Klein and Marcus evidence concerning the "splitter cabinets" that duplicate for the government the flow of data through AT&T's facilities: "Current and former intelligence officials say telecom companies[] ... are giving the government unlimited access to a copy of the flow of communications, through a network of switches at U.S. telecommunications hubs that duplicate all the data running through it." *Id.* at 3. The article confirms that the NSA's domestic electronic surveillance is not limited to communications with terrorists overseas: "[F]or instance ... the government's spy systems may be directed to collect and analyze all electronic communications into and out of the city [of Detroit]." *Id*. at 2. "[S]ome intelligence officials now say the broader NSA effort amounts to a driftnet." *Id* at 4-5.

IV. The Government's Notion That Section 1806(f) Does Not Speak Directly To The Use Of Evidence That Would Otherwise Be Subject To The State Secrets Privilege Is Meritless

As demonstrated above, section 1806(f) by its plain terms applies whenever in response to a party's "motion or request … to discover or obtain applications or orders or other materials relating to electronic surveillance" the government interposes an assertion that "disclosure or an adversary hearing would harm the national security of the United States." § 1806(f). It does so

[8] Available at http://online.wsj.com/public/article_print/SB120511973377523845.html.

"notwithstanding any other law." *Id*.

The government argues that, notwithstanding the clarity of Congress' language and purpose, Congress did not really mean what it said, and that the state secrets privilege preempts section 1806(f) and not vice versa. The government's position in a nutshell is that it does not ultimately matter what section 1806(f) provides because the Executive retains the state secrets privilege as a trump card and can play that card whenever it wishes to block the Judiciary from applying section 1806(f) as Congress has directed. The government's position is meritless.

The starting point for this analysis is the Ninth Circuit's reaffirmation that "[t]he state secrets privilege is a common law evidentiary privilege," *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1196 (9th Cir. 2007), the same ruling this Court made in its *Hepting* Order. *Hepting*, 439 F.Supp.2d at 980 ("The state secrets privilege is a common law evidentiary rule."); *accord*, *Kasza v. Browner*, 133 F.3d 1159, 1165 (9th Cir. 1998) ("The state secrets privilege is a common law evidentiary privilege …."). That ruling is not only controlling Ninth Circuit authority but is law of the case in these proceedings.

As a federal common law privilege, the state secrets privilege is subject to preemption by congressional legislation that "speaks directly" to the question otherwise answered by federal common law, as the Al-Haramain plaintiffs explain in their opposition at 9 to 12. Here, there can be no doubt that Congress hit the mark it aimed at when it enacted section 1806(f).

Congress' purpose in section 1806(f) is what its text states it to be: to provide a method for a "determination of whether the surveillance of the aggrieved person was lawfully conducted" in those instances where the government tells the court that "disclosure or an adversary hearing would harm the national security of the United States." § 1806(f). The government said exactly that in invoking the state secrets privilege with respect to materials relating to the surveillance in the Hepting action: "[D]isclosure of the information covered by these privilege assertions would cause exceptionally grave damage to the national security of the United States." Dkt. # 124, attachment 1 & 2 at 2, in No. 06-0672. There is no material difference between the content of the assertion by the government in Hepting and the content of the Attorney General assertion that triggers 1806(f).

The government's notion that Congress in one and the same act both called section 1806(f) into being and preserved the common law state secrets privilege unchanged is logically incoherent, because they both speak to the same issue and are fundamentally irreconcilable. The whole point of section 1806(f) is to remove the ability of the Executive to unilaterally forestall a determination of the legality of electronic surveillance by withholding from judicial scrutiny the materials relating to the surveillance, the very power it might otherwise have under the state secrets privilege. Section 1806(f)'s purpose was to put electronic surveillance under the law, not to preserve an escape hatch to keep it above the law; it thereby fulfills Congress' larger purpose of making FISA and Title III the "exclusive means" by which electronic surveillance is conducted. The government suggests no plausible reason, except perhaps sheer incompetence, why Congress would have bothered to create a stillborn statute like the one the government imagines section 1806(f) to be.

Likewise, the government's notion that Congress could not successfully preempt the state secrets privilege unless the *Congressional Record* somewhere records a shamanistic incantation of the words "states secrets privilege" in connection with section 1806(f) is a myth of its own invention. The inquiry into preemption of common law by statute is a practical, not a formalistic, one, as *Kasza* illustrates. The statute in *Kasza*, which the Ninth Circuit held did not preempt the state secrets privilege, was one that comprehensively regulated the operations of garbage dumps and provided for the public release of reports submitted by garbage dumps to the government. *Kasza*, 133 F.3d at 1167-68. The statute authorized the president to exempt federal garbage dumps from all the regulatory requirements of the statute if it was in the "paramount national interest," whether or not that interest had anything to do with the national security. Unlike section 1806(f), the exemption had nothing to do with judicial proceedings or the production of evidence pursuant to judicial process, and did not purport to create a privilege to withhold or limit the disclosure evidence or a protocol for the court to safely receive secret evidence.

The Ninth Circuit concluded there was no preemption by making a practical comparison of the highly different purposes of the garbage-dump statute and of the state secrets privilege: "the state secrets privilege and [the garbage-dump statute] have different purposes: one is an evidentiary privilege that allows the government to withhold sensitive information within the context of litigation; the other allows the President to exempt a federal facility from compliance with [the garbage dump] regulatory regime." *Kasza*, 133 F.3d at 1167-68. The idea that Congress had created the power to exempt federal garbage dumps from complying with dump regulations for the ulterior purpose of regulating the admissibility of evidence in unforeseeable litigation far down the road was simply too far-fetched.

Here, by contrast, the state secrets privilege and section 1806(f) do share a common, unified purpose: they both regulate the evidentiary and litigation consequences that flow from the government's assertion that the national security would be harmed by the disclosure, otherwise compelled by the rules of discovery and evidence, of a particular category of evidence.

The *Kasza* court also noted that the state secrets privilege and the garbage-dump statute only overlapped partially at the fringes, a tenuous connection making it unlikely that Congress' intent had been "to replace the government's evidentiary privilege to withhold sensitive information in litigation by providing an exemption from the [garbage-dump statute's] regulation of hazardous waste." *Id*. at 1168. Here, however, the state secrets privilege completely encompasses section 1806(f): *Every* instance in which the Attorney General triggers the section 1806(f) protocol by asserting that the disclosure of evidence "would harm the national security" is an instance in which, absent section 1806(f), the state secrets privilege otherwise could be invoked.[9]

V. Congress Has The Authority To Regulate The Use In Litigation Of Information That The Executive Asserts Is A State Secret

Given that section 1806(f) does apply to materials relating to electronic surveillance that would otherwise be subject to the state secrets privilege, the government is left with nothing more than the argument, only hinted at in its motion, that the Executive can disregard section 1806(f) notwithstanding the statute's applicability.

Any suggestion that Congress may lack the constitutional power to regulate the use of surveillance evidence in judicial proceedings because to do so would intrude on the President's war

[9] In arguing against preemption of the state secrets privilege by section 1806(f), the government is thereby arguing that evidence to which section 1806(f) applies is not evidence to which the state secrets privilege applies. This is an untenable position, for its unstated but necessary premise is that surveillance evidence that would, if disclosed, harm the national security for purposes of section 1806(f) somehow would *not*, if disclosed, harm the national security for purposes of the state secrets privilege. The government can give no rational basis for such a distinction.

powers is meritless. As the Supreme Court has recognized repeatedly, the war powers are "powers granted *jointly* to the President and Congress." *Hamdan v. Rumsfeld*, 126 S.Ct. 2749, 2773 (2006) (emphasis added). For example, the President is the "Commander in Chief" under article II, but he can only command such forces as Congress "raise[s] and support[s]" under article I, § 8, cl. 12.

Of particular significance here is Congress' power "To make Rules for the Government and Regulation of the land and naval Forces." Const., art. I, cl. 14. However far the Executive's power under article II to conduct intelligence surveillance may extend, clause 14 of article I gives Congress a coextensive power to "make Rules for the Government and Regulation" of that surveillance, including the power to determine when and how "materials relating to electronic surveillance" the Executive conducts should be made available for use in litigation. *See Hamdan*, 126 S.Ct. at 2774 n.23, 2786 (statute governing trials of enemies enacted pursuant to Congress' war powers preempts a different system of trial by commission established by the Executive).

Likewise Congress' power to prescribe rules for judicial proceedings allows it to regulate the state secrets privilege and establish alternative proceedings like section 1806(f). *See* Const. art. I, § 8, cl. 9 (power "To constitute Tribunals inferior to the supreme Court"), cl. 18 ("To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof [e.g., the Judicial Department]."); Const. art. III, § 1 (Congress' power to "ordain and establish" inferior courts).

When Congress affirmatively exercises these powers, the Executive's power is at its "lowest ebb," in the classic tripartite formulation of *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring). Throughout our history, the Supreme Court has reaffirmed Congress' power to "make Rules for the Government and Regulation" of the Executive's war powers. *See, e.g., Little v. Barreme*, 6 U.S. 170, 178-79 (1804) (Because Congress had imposed limitations on searches and seizures by naval vessels during war, Executive could not authorize searches and seizures beyond the scope of what Congress authorized).

Most recently, the Supreme Court strongly reaffirmed Congress' coequal war power in *Hamdan*, 126 S.Ct. at 2774 n.23, stating: "Whether or not the President has independent power, absent congressional authorization, … he may not disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring). The Government does not argue otherwise."

In *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), the Court rejected the notion that the Executive's national security powers can restrict the constitutional powers of the other coequal branches. The plurality noted that the claim of Executive supremacy

> cannot be mandated by any reasonable view of separation of powers, as this approach serves only to *condense* power into a single branch of government. We have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens. *Youngstown Sheet & Tube*, 343 U.S., at 587. Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, *it most assuredly envisions a role for all three branches when individual liberties are at stake*.

Hamdi, 542 U.S. at 535-36 (plurality opinion) (first emphasis original, second emphasis added).

When at its lowest ebb, "[c]ourts can sustain exclusive presidential control in such a case only by disabling the Congress from acting upon the subject." *Youngstown*, 343 U.S. at 637-38 (Jackson, J., concurring). Here, Congress is not disabled from acting on the subject of electronic surveillance of American citizens within the United States, and so any claim of Executive power to disregard section 1806(f) fails.

"No penance would ever expiate the sin against free government of holding that a President can escape control of executive powers by law through assuming his military role." *Youngstown*, 343 U.S. at 646 (Jackson, J., concurring). Thus, there is no doubt that "the Executive is bound to comply with the Rule of Law that prevails in this jurisdiction." *Hamdan*, 126 S.Ct. at 2798. The "Rule of Law that prevails in this jurisdiction" and in these actions includes section 1806(f).

CONCLUSION

For the foregoing reasons, the Court should hold that section 1806(f) preempts the state secrets privilege with respect to the subject matter of materials and information relating to electronic surveillance in civil actions seeking relief from unlawful surveillance.

DATED: April 7, 2008

Respectfully submitted,

/s/ Richard R. Wiebe
Richard R. Wiebe

Laurence F. Pulgram (CSB No. 115163)
Jennifer Kelly (CSB No. 193416)
Candace Morey (CSB No. 233081)
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350

COUNSEL FOR AMICI;
ATTORNEYS FOR PLAINTIFFS IN CAMPBELL v. AT&T AND IN RIORDAN v. VERIZON COMMUNICATIONS INC.

Ann Brick (CSB No. 65296)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437

COUNSEL FOR AMICI;
ATTORNEYS FOR PLAINTIFFS IN CAMPBELL v. AT&T AND IN RIORDAN v. VERIZON COMMUNICATIONS INC.

Richard R. Wiebe
LAW OFFICE OF RICHARD R. WIEBE
425 California Street
Suite 2025
San Francisco, CA 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382

COUNSEL FOR AMICI;
ATTORNEY FOR
AT&T CLASS PLAINTIFFS

ELECTRONIC FRONTIER FOUNDATION
Cindy A. Cohn, Esq. (SBN 145997)
Lee Tien, Esq. (SBN 148216)
Kurt Opsahl, Esq. (SBN 191303)
Kevin S. Bankston, Esq. (SBN 217026)
Corynne McSherry, Esq. (SBN 221504)
James S. Tyre, Esq. (SBN 083117)
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993

COUNSEL FOR AMICI;
ATTORNEYS FOR
AT&T CLASS PLAINTIFFS AND
CO-CHAIR OF PLAINTIFFS' EXECUTIVE COMMITTEE

Additional Plaintiffs' Counsel on Executive Committee and Liaison Counsel:

ROGER BALDWIN FOUNDATION OF ACLU
HARVEY GROSSMAN
ADAM SCHWARTZ
180 North Michigan Avenue
Suite 2300
Chicago, IL 60601
Telephone: (312) 201-9740
Facsimile: (312) 201-9760

PLAINTIFFS' COUNSEL FOR AT&T SUBSCRIBER CLASS AND CO-CHAIR OF PLAINTIFFS' EXECUTIVE COMMITTEE

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
ELIZABETH J. CABRASER
BARRY R. HIMMELSTEIN
ERIC B. FASTIFF
275 Battery Street, 30th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008

PLAINTIFFS' COUNSEL FOR MCI SUBSCRIBER CLASS

MOTLEY RICE LLC
RONALD MOTLEY
DONALD MIGLIORI
JODI WESTBROOK FLOWERS
JUSTIN KAPLAN
28 Bridgeside Boulevard
P.O. Box 1792
Mt. Pleasant, SC 29465
Telephone: (843) 216-9163
Facsimile: (843) 216-9680

PLAINTIFFS' COUNSEL FOR VERIZON SUBSCRIBER CLASS AND MISCELLANEOUS SUBSCRIBER CLASSES

GEORGE & BROTHERS, L.L.P.
R. JAMES GEORGE, JR.
DOUGLAS BROTHERS
1100 Norwood Tower
114 W. 7th Street
Austin, Texas 78701
Telephone: (512) 495-1400
Facsimile: (512) 499-0094

PLAINTIFFS' COUNSEL FOR CINGULAR SUBSCRIBER CLASS

THE MASON LAW FIRM, PC
GARY E. MASON
NICHOLAS A. MIGLIACCIO
1225 19th St., NW, Ste. 500
Washington, DC 20036
Telephone: (202) 429-2290
Facsimile: (202) 429-2294

PLAINTIFFS' COUNSEL FOR SPRINT SUBSCRIBER CLASS

ILANN M. MAAZEL
EMERY CELLI BRINCKERHOFF & ABADY LLP
75 Rockefeller Plaza, 20th Floor
New York, NY 10019
Telephone: (212) 763-5000
Facsimile: (212) 763-5001

PLAINTIFFS' COUNSEL IN SHUBERT V. BUSH

CENTER FOR CONSTITUTIONAL RIGHTS
SHAYANA KADIDAL
666 Broadway, 7th Floor
New York, NY 10012
Telephone: (212) 614-6438
Facsimile: (212) 614-6499

PLAINTIFFS' COUNSEL IN CENTER FOR CONSTITUTIONAL RIGHTS v. BUSH

BRUCE I AFRAN, ESQ.
10 Braeburn Drive
Princeton, NJ 08540
609-924-2075

PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS

KRISLOV & ASSOCIATES, LTD.
CLINTON A. KRISLOV
20 North Wacker Drive
Suite 1350
Chicago, IL 60606
Telephone: (312) 606-0500
Facsimile: (312) 606-0207

PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS

NATIONAL LAWYERS GUILD
MICHAEL AVERY
c/o Suffolk Law School
120 Tremont Street
Boston, MA 02108
Telephone: (617) 573-8551
Facsimile: (617) 305-3090

PLAINTIFFS' COUNSEL IN CENTER FOR CONSTITUTIONAL RIGHTS v. BUSH

MAYER LAW GROUP LLC
CARL J. MAYER
66 Witherspoon Street, Suite 414
Princeton, New Jersey 08542
Telephone: (609) 921-8025
Facsimile: (609) 921-6964

PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS

LISKA, EXNICIOS & NUNGESSER ATTORNEYS-AT-LAW
VAL PATRICK EXNICIOS
One Canal Place, Suite 2290
365 Canal Street
New Orleans, LA 70130
Telephone: (504) 410-9611
Facsimile: (504) 410-9937

PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS

THE LAW OFFICES OF STEVEN E. SCHWARZ, ESQ.
STEVEN E. SCHWARZ
2461 W. Foster Ave., #1W
Chicago, IL 60625
Telephone: (773) 837-6134

PLAINTIFFS' COUNSEL FOR BELLSOUTH SUBSCRIBER CLASS